Memorandum of Understanding

Between FSA

And

[Organization B]

[Date Here]

Version 1.0

For Official Use Only

[Delete everything inside square brackets [ ] throughout this template including this comment after reading. Replace the brackets and their contents with appropriate information.]
SUPERSEDES: [None or document title and date]

INTRODUCTION

Federal policy requires federal agencies to establish interconnection agreements. Specifically, *Office of Management and Budget (OMB) Circular A-130, Appendix III*, requires agencies to obtain written management authorization before connecting their IT systems to other systems, based on an acceptable level of risk. The written authorization should define the rules of behavior and controls that must be maintained for the system interconnection, and it should be included in the organization's system security plan. This MOU was prepared using and following guidelines set forth in the National Institute of Standards and Technology (NIST) Special Publications (SP) 800-47 *Security Guide for Interconnecting Information Technology System*s, September 2002, which defines the responsibilities of the participating organizations and, NIST 800-18 *Guide for Developing Security Plans for Information Technology System*s, December 1998. The disaster recovery section promotes compliance with the Government Information Security Reform Act (GISRA) and meets Certification and Accreditation criteria. The supporting Interconnection Security Agreement (ISA) specifies the technical and security requirements of the interconnection.

PURPOSE

The purpose of this memorandum is to establish a management agreement between FSA and [Organization B] regarding the development, management, operation, and security of a connection between [System A], owned by FSA, and [System B], owned by [Organization B]. This agreement will govern the relationship between FSA and [Organization B], including designated managerial and technical staff, in the absence of a common management authority.

BACKGROUND

It is the intent of both parties to this agreement to interconnect the following information technology (IT) systems to exchange data between [ABC database] and [XYZ database]. FSA requires the use of [Organization B]'s [ABC database], and [Organization B] requires the use of FSA's [XYZ database] [change this sentence as appropriate]. The expected benefit of the interconnection is to expedite the processing of data associated with [Project R] within prescribed timelines.

Each IT system is described below:

- [SYSTEM A]
  - Name:
  - Function:
  - Location of system hardware:
  - Description of data to be exchanged, including sensitivity or classification level:

Category	Definition	Sensitivity Rating
Confidentiality	Protection from unauthorized disclosure.	
Integrity	Protection from unauthorized, unanticipated, or unintentional modification.	
Availability	Available on a timely basis to meet mission requirements or to avoid substantial loses.	

- [SYSTEM B]
  - Name:
  - Function:
  - Location of system hardware:
  - Description of data to be exchanged, including sensitivity or classification level:

Category	Definition	Sensitivity Rating
Confidentiality	Protection from unauthorized disclosure.	
Integrity	Protection from unauthorized, unanticipated, or unintentional modification.	
Availability	Available on a timely basis to meet mission requirements or to avoid substantial loses.	

COMMUNICATIONS

Rules of Behavior
Both parties will abide by the policies and procedures set forth by the Department of Education, including the *FSA Information Technology Security and Privacy Policy*.

General Communications
Frequent formal communications are essential to ensure the successful management and operation of the interconnection. The parties agree to maintain open lines of communication between designated staff at both the managerial and technical levels. The communication is expected to be professional, courteous, and mutually respectful to promote a successful partnership and interconnection. All communications described herein must be conducted in writing unless otherwise noted.

The owners of [System A] and [System B] agree to designate and provide contact information for technical leads for their respective system, and to facilitate direct contacts between technical leads to support the management and operation of the interconnection. To safeguard the confidentiality, integrity, and availability of the connected systems and the data they store, process, and transmit, the parties agree to provide notice of specific events within the time frames indicated below:

- **Security Incidents:** Technical staff will notify their System Security Officer (SSO) when a security incident(s) is detected that would affect the other system. The SSO will contact the designated counterparts by personal contact, telephone, Blackberry, pager or e-mail so the other party may take steps to determine whether its system has been compromised and to take appropriate security precautions. The system owner will receive formal notification in writing within five (5) business days after detection of the incident(s).

- **Disasters and Other Contingencies:** Technical staff will notify their System Security Officer (SSO) in the event of a disaster or other contingency that disrupts the normal operation of one or both of the connected systems and that would affect the other system. The SSO will contact the designated counterparts by personal contact, telephone, Blackberry, pager or e-mail. Once notification occurs, both parties should follow the applicable procedures documented in the appropriate system contingency plan.

- **Material Changes to System Configuration:** Planned technical changes to the system that will affect data exchange will be reported to the other party's technical staff before such changes are implemented. The initiating party agrees to conduct a risk assessment based on the new system architecture to ensure that there will not be significant risks introduced to the other party with the changes.

- **New Interconnections:** The initiating party will notify the other party at least one (1) month *before* it connects its IT system with any other IT system, including systems that are owned and operated by third parties, such as contractors or vendors.

- **Personnel Changes:** The parties agree to provide notification of the separation or long-term absence of their respective system owner or technical lead. In addition, both parties will provide notification of changes in point of contact information.

INTERCONNECTION SECURITY AGREEMENT

The technical details of the interconnection will be documented in an Interconnection Security Agreement (ISA). The parties agree to work together to develop the ISA, which must be signed by both parties before the interconnection is activated. Proposed changes to either system or the interconnecting medium will be reviewed and evaluated to determine the potential impact on the interconnection. The ISA will be renegotiated before changes are implemented. Signatories to the ISA shall be the designated approval authority for each system.

SECURITY

Both parties agree to work together to ensure the joint security of the connected systems and the data they store, process, and transmit, as specified in the ISA. For example, respective system security plans, contingency plans, disaster recovery plans, and other information relative to the interconnection should be closely coordinated and documentation shared with corresponding system stakeholders as appropriate.

Each party certifies that its respective system is designed, managed, and operated in compliance with all relevant federal laws, regulations, and policies.

COST CONSIDERATIONS

Both parties agree to equally share the costs of the interconnecting mechanism and/or media, but no such expenditures or financial commitments shall be made without the written concurrence of both parties. Modifications to either system that are necessary to support the interconnection are the responsibility of the respective system owners' organization.

TIMELINE

This agreement will remain in effect for one (1) year after the last date on either signature in the signature block below. After one (1) year, this agreement will expire without further action. If the parties wish to extend this agreement, they may do so by reviewing, updating, and reauthorizing this agreement. The newly signed agreement should explicitly supersede this agreement, which should be referenced by title and date. If one or both of the parties wish to terminate this agreement prematurely, they may do so upon 30 days' advanced notice or in the event of a security incident that necessitates an immediate response.

SIGNATORY AUTHORITY

I agree to the terms of this Memorandum of Understanding (or Agreement).

FSA Official	**[Organization B's] Official**
[Name]	**[Name]**
[Title]	**[Title]**
_____	_____
(Signature Date)	(Signature Date)